True Random Number Generator Harvesting Entropy from Stochastic Switching Time of MTJ

應用於亂數產生器之 MTJ 的隨機轉換時間

組別 ： A64　　指導教授 ： 張孟凡　　組員 ： 李睿

Abstract

亂數產生器在數據傳輸中有著關鍵作用，由於現今的傳輸都會先將資料加密，而加密會需要用到金鑰，而這金鑰就可以從亂數產生器生成，因此亂數產生器的好壞可以決定到資料傳輸的安全程度。在大多數情況下，亂數是由 PRNG（偽亂數產生器）生成的，但是這種發生器有其局限性[1]，因此提出了 TRNG（真亂數產生器）。它通過其隨機的物理屬性生成隨機數，而些物理特性會表現在當出現干擾，像是熱干擾或電壓干擾時。干擾會影響數位電路的輸出。因此，我們稱干擾作為「熵」的來源，可用於設計 TRNG，而在此次實驗提出了一個 TRNG 的架構。

Implementation

在本實驗中，將使用 MRAM 寫入資料的時間來實現 MRAM TRNG，如 Fig.1 所示，在這次實驗中，使用一個計數器來計算 MRAM 狀態從 AP 變為 P，即為將 MRAM 裡存取的資料從 0 寫至 1 所經過的時間，Fig.2 為此次實驗架構圖。當資料寫入完成時，BL 電壓會上升，stop 電壓下降，counter 停止計算，如 Fig.3。計數器中的許多位元都是隨機數，然而有些則是離標準差了一點便可成為隨機數，因此為了達到更好的性能，此次實驗對這些未能達標的位元使用 XOR 邏輯閘，而結果也確實顯示，此方法可以使得他們成為亂數，提高亂數的產率，且同時節省了面積。

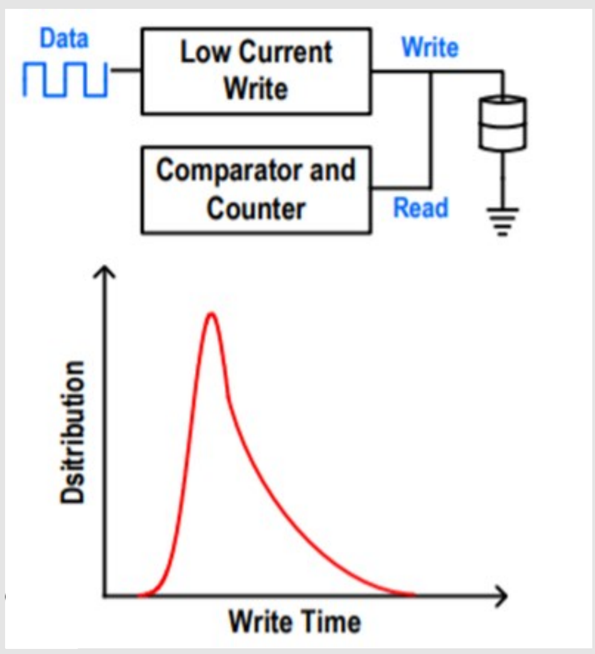

Fig.1 系統概念圖

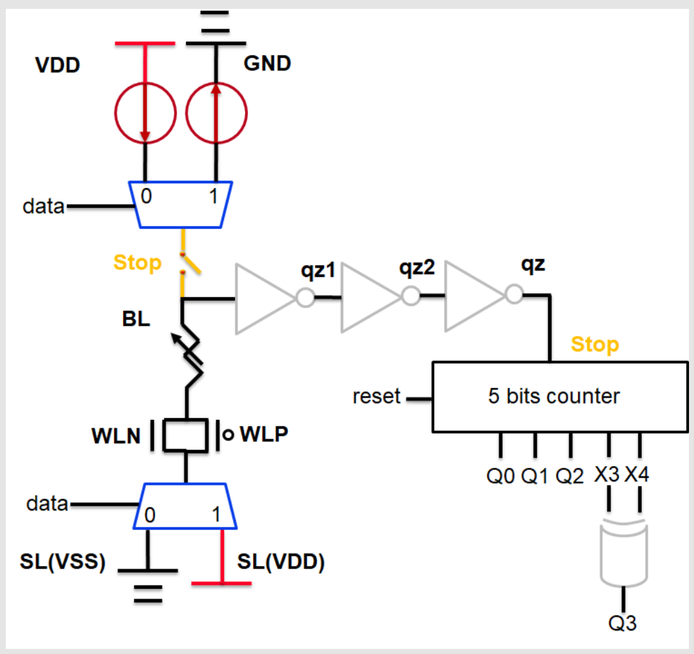

Fig.2 系統架構圖

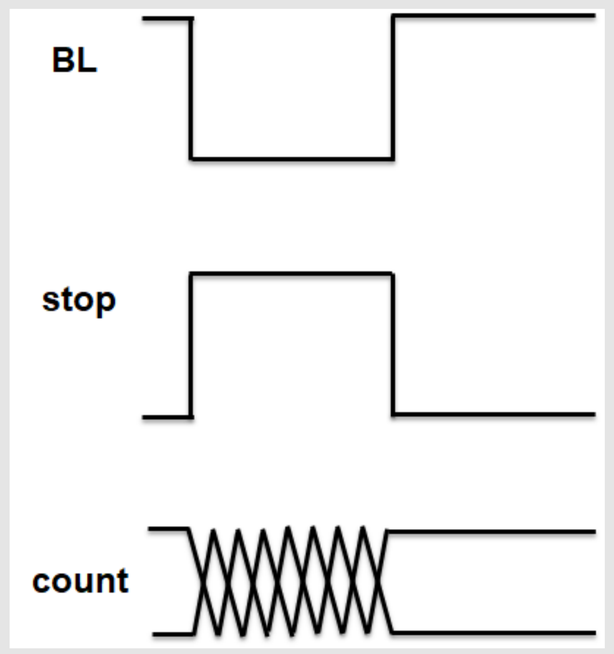

Fig.3 波型圖示意圖

Result

5bit counter 有 XOR 可以在較少的面積下，產生比 6bit counter 無 XOR 多的亂數，因此可以知道添加 XOR 可以讓亂數的產生更有效率。Fig.5 是將產生的亂數去跑 NIST 800-22 得出的結果。

不同位元數的 counter	有無 XOR	Number of usable bits
4bits counter	無 XOR	3
	有 XOR	3
5bits counter	無 XOR	3
	有 XOR	4
6bits counter	無 XOR	3
	有 XOR	4

Fig.4 亂數產生結果

Test	P value		Proportion		Success/Fail
Frequency	0.53		1		Success
Block Frequency	0.35		1		Success
Runs	0.06		1		Success
Longest Run of Ones	0.53		1		Success
FFT	0.35		1		Success
Approximate Entropy			1		Success
Cumulative Sums	0.035	0.067	1	1	Success
Serial			1	1	Success
Non-overlapping Template Matching	Pass 97.3% of the sub-test				

Fig.5 亂數亂度測試結果

Conclusion

此次實驗結果有達到預期成果，產生的數為亂數，且 XOR 能使 counter 的每一位元與 TRNG 的面積更有效率的使用。

Reference

[1] K. Yang et al., “A 28 nm integrated true random number generator harvesting entropy from MRAM,” in Symp. VLSI Circuits Dig. Tech. Papers, pp. 171–172, Jun. 2018.